CRIMINAL JUSTICE CONNECTIONS

March/April 2017
Volume 24 Issue 4

An employee publication of the
Texas Department of Criminal Justice

Policies and Benefits

Upgrade data security with easy-to-remember passphrases

In recent years, passphrases have begun to replace passwords as a method of user authentication. Some agency computer systems already use passphrases and the Information Technology Division is currently evaluating how to migrate key TDCJ systems, such as the mainframe, to allow for the use of passphrases in the future. There's no cause for concern, though, as switching from using passwords to passphrases can be easy if done correctly.

A password is an arbitrary string of typographic characters used to identify a computer user before they are allowed access to secure information. Everyone who uses a computer on a regular basis is likely to be familiar with username and password procedures. Many current TDCJ computer systems require passwords of up to ten characters and prohibit use of dictionary words, proper names, user names or ID numbers. Users are also required to change passwords on a regular basis.

A passphrase is similar to a password in that both are used to prove identity, but a well-designed passphrase is not only more secure than a password, it can be easier to remember.

The primary benefit of a passphrase is the increased number of potential typographic character (letters, numbers and symbols) combinations when compared to a single password. Passphrases might include twenty to thirty characters, or more. Since a passphrase is a sentence, even a complex character combination can be both secure and simple to use.

Take the sample passphrase:

RememberThe@l@mo!

First, don't use this published phrase as a real passphrase. It's only being used as an example.

Notice that this multiword passphrase is easy to remember and conforms to the agency's complexity requirements. Attempts to hack into this system by entering single words from a dictionary are doomed to fail. Also, note that even though the passphrase contains three words, no spaces are used; eliminating the spaces between words improves the likelihood that the computer's authentication mechanism will correctly read your passphrase text.

Devising and remembering a passphrase may at first seem like a lot of trouble, but keep in mind that the more words and characters you put into your passphrase, the harder it is to hack. A well-designed passphrase will improve data security and can be as easy to use as a traditional password.